

REMARKS

Claims 1-26 are pending in the application. Claims 1-17 and 26 are rejected. Applicant thankfully acknowledges the Examiner's indication that claims 18-25 include allowable subject matter and would be allowable if rewritten as suggested in the Office Action. However, Applicant respectfully traverses the claim rejections and requests reconsideration of the rejections based on the following remarks.

Claim Rejections- 35 U.S.C. §102

Claims 1-15 are rejected as being anticipated by Hashimoto (US. 4,907,275). Applicant respectfully disagrees and submits that at the very least, claims 1, 7, 11, 13, and 15 are patentably distinct and patentable over Hashimoto. Fundamentally, the claimed inventions differ in function and purpose than the methods and teachings in Hashimoto as cited by the Examiner.

In general, the claimed inventions are directed to systems and methods for efficient data encryption, which are designed to remove redundancies of conventional systems in which the same plaintext block is read from memory two times, once for a first mode (e.g., CTR encryption) and once for a second mode (e.g., CBC encryption). For instance, claim 1 recites *a method for encrypting data*, comprising the steps of:

reading a plaintext data block from a memory;
storing the plaintext data block in an input buffer;
encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext;
storing the first ciphertext in an output buffer; and
encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext.

In formulating the rejection of claim 1, the Examiner essentially relies on Hashimoto's teachings in Col. 3, lines 16-30, and Fig. 1 as disclosing the process of claim 1, in particular, as disclosing encrypting a buffered plaintext data block using a first mode and a second mode. However, Applicant respectfully disagrees with the Examiner's findings.

Indeed, Hashimoto discloses (in the cited sections) an encryption process (such as depicted in FIG. 1) in which a sequence of 8 plaintext data blocks A-H are stored in an input buffer (14), and then accessed and encrypted by an encryption system (15) in a way that the encrypted text block sequence comprising corresponding encrypted plaintext blocks A', B', D', G' and H' and non-encrypted plaintext blocks, C, E, and F, can be stored in an output buffer (16) in a sequence A', B', C, D', E, F, G' and H' at addresses corresponding to the addresses of the plaintext block sequence A, B, C, D, E, F, G, and H stored in the input buffer (14).

In view of the above, although Hashimoto arguably teaches storing a sequence of plaintext data blocks in an input buffer (14), there is no teaching in the cited sections of *encrypting a plaintext data block in the input buffer using a first mode to generate a first ciphertext, and encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext*, within the scope and context of claim 1. Indeed, it is *wholly* unclear how the Examiner interprets Hashimoto as teaching these claim limitations given that the cited sections relied on Hashimoto are *utterly devoid* of any teaching of encrypting a plaintext data block in the input buffer using a first mode and encrypting the same plaintext data block using a second mode, as recited in claim 1.

Moreover, the basis for the rejection of claim 1 is clearly contradicted, and wholly undermined, by the Examiner's acknowledgment on the bottom of p. 5 of the Office Action where the Examiner admits that Hashimoto "is silent on the capability of using a plurality of

modes of operation in the encryption system.” This admission renders the rejection of claim 1 legally deficient on its face.

For at least the above reasons, Applicant respectfully asserts that the Office Action fails to set forth a *prima facie* case of anticipation of claim 1 based on the teachings of Hashimoto. Moreover, given that the rejections of claims 7, 13 and 15 are based on the same rationale given for claim 1, it is submitted that no prima facie case of anticipation has been established for claims 7, 13 and 15 based on Hashimoto for at least the same reasons given above for claim 1. In this regard, claims 1, 7, 13, 15 and corresponding dependent claims are patentable over Hashimoto.

Moreover, with regard to claims 11-12, at the very least, claim 11 is not anticipated by Hashimoto. In formulating the rejection of claim 11, the Examiner cites Col. 1, lines 52-58 of Hashimoto (which discloses a conventions CBC encryption/decryption mode in FIG. 11), but offers no supporting explanation as to how Hashimoto’s teachings meet the limitations of claim 11. In any event, Applicant respectfully asserts that the rejection of claim 11 is legally deficient as a matter of law, in that Hashimoto clearly discloses one mode, i.e., CBC . In this regard, there is no basis for finding that Hashimoto teaches the claim limitations of , e.g.,

decrypting the ciphertext data block in the input buffer using a first mode to generate a plaintext;

storing the plaintext in the input buffer, an output buffer or both; and

encrypting the plaintext in the input buffer or the output buffer using a second mode to generate a ciphertext, as recited in claim 11.

Therefore, the Office Action fails to present a *prima facie* case of anticipation of claims 11 and 12. Accordingly, withdrawal of the anticipation rejections is requested.

Claim Rejections- 35 U.S.C. §103

Claims 16-17 and 26 are rejected as being unpatentable over Hashimoto in view of Matchett (US. 7,092,525). The rejections are respectfully traversed.

At the very least, the combination of Hashimoto and Matchett is legally deficient to establish a prima facie case of obviousness against claim 16. At the very least, the combination of Hashimoto and Matchett does not teach or suggest, e.g., *an encryption module that encrypts the block of data stored in the input buffer using one of a plurality of modes of operation supported by the encryption module including a CTR (counter) mode, CBC (cipher block chaining) mode and CCM (CTR and CBC-MAC (message authentication code) mode*, as recited in claim 16. The reasons are as follows.

The Examiner acknowledges that Hashimoto does not teach an encryption system with multiple modes of operation. Instead, the Examiner relies on Matchett as teaching an improved DES cryptographic system for cryptographic protection of data through modifications of the cipher function and cipher key as specified in the DES standard (Col. 1, lines 13-51). Applicant respectfully asserts that the Examiner's reliance on Matchett in this regard is essentially misplaced and irrelevant, because Matchett is only concerned with the DES cryptography standard and related modes such as CBC, ECB, CFB and OFB.

In particular, Matchett does not teach or fairly suggest a multiple mode encryption system including CTR or CCM modes as claimed, because these modes are not compatible with DES. In fact, it is extremely well known that CCM is an AES mode of operation, and that the AES cryptography standard is much different from the DES cryptography standard, as is understood

by those of ordinary skill in the art. As such, there is no teaching in Matchett of a multi mode DES system including CTR and CCM modes.

Furthermore, it should be fundamentally clear that Hashimoto is only concerned with DES cryptography. The Examiner contends that Hashimoto teaches an encryption module that encrypts a block of data using one of a plurality of modes of operation including CTR and CCM. This finding is clearly erroneous as a matter of fact because the AES standard and CCM mode where not in existence at the time of the US filing of Hashimoto's application (i.e., May 18, 1998). Therefore, there is no basis for any of the Examiner's findings with regard to Hashimoto teaching AES modes such as CCM.

Therefore, the combined teachings of Hashimoto and Matchett do not teach or suggest, but rather teach away from, a multi-mode encryption system that includes a CCM mode, for example. As such, claim 16 and corresponding dependent claims 17 and 26 are patentable over the combination of Hashimoto and Matchett. Withdrawal of the obviousness rejections is respectfully requested.

Respectfully submitted,



Frank DeRosa
Reg. No. 43,584
Attorney for Applicant

F. Chau & Associates, LLC
130 Woodbury Road
Woodbury, NY 11797
TEL.: (516) 692-8888
FAX: (516) 692-8889